IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF PENNSYLVANIA

MALINDA S. SMIDGA, individually and on behalf of all others similarly situated, Plaintiff, v. SPIRIT AIRLINES, INC., Defendant.	Case No. 2:22-cv-01578-MJH **JURY TRIAL DEMANDED**
FRANCES CURD, individually and on behalf of all others similarly situated, Plaintiff, v. SPIRIT AIRLINES, INC., Defendant.	Case No. 2:23-cv-00895-MJH **JURY TRIAL DEMANDED**
KAYLA MANDENG, individually and on behalf of all others similarly situated, Plaintiff, v. SPIRIT AIRLINES, INC., Defendant.	Case No. 2:23-cv-00784-MJH **JURY TRIAL DEMANDED**

CONSOLIDATED AMENDED COMPLAINT - CLASS ACTION

Plaintiffs Malinda S. Smidga, Frances Curd, and Kayla Mandeng ("Plaintiffs"), individually and on behalf of all others similarly situated, hereby file this consolidated amended class action complaint against Defendant Spirit Airlines, Inc. ("Defendant" or "Spirit"), and in support thereof allege the following:

INTRODUCTION

1. This is a class action brought against Spirit for wiretapping the electronic communications of visitors to its website, www.spirit.com. Spirit procures third-party vendors, such as FullStory, to embed snippets of JavaScript computer code ("Session Replay Code") on Spirit's website, which then deploys on each website visitor's internet browser for the purpose of intercepting and recording the website visitor's electronic communications with Spirit's website, including their mouse movements, clicks, keystrokes (such as text being entered into an information field or text box), URLs of web pages visited, and/or other electronic communications in real-time ("Website Communications"). The Session Replay Code procured by Defendant surreptitiously and instantaneously intercepted, stored, and recorded everything Plaintiffs and the Class Members did on Defendant's website, *e.g.*, what they searched for, what they looked at, the information they input, and what they clicked on for the entire duration of their visit.

2. These third-party vendors, such as FullStory, (collectively, "Session Replay Providers") create and deploy the Session Replay Code at Spirit's direction, and capture and store the Website Communications of each website visitor.

3. After intercepting and capturing the Website Communications, Spirit and the Session Replay Providers use those Website Communications to recreate website visitors' entire visit to www.spirit.com. The Session Replay Providers can create, using the swaths of website users' data they collect from users' browsing sessions and browsing devices, a video replay of the

user's behavior on the website and provide it to Spirit. Spirit's procurement of the Session Replay Providers to secretly deploy the Session Replay Code results in the electronic equivalent of "looking over the shoulder" of each visitor to Spirit's website for the entire duration of their interaction with Defendant's website.

4. Defendant knowingly, willfully, and intentionally procured the interception of, and used, the electronic communications at issue without the knowledge or prior consent of Plaintiffs or the Class Members. Defendant did so for its own financial gain and in violation of Plaintiffs' and the Class Members' substantive legal privacy rights under the various wiretapping laws and other state statutes and the common law.

5. The Session Replay Code utilized by Defendant is not a traditional website cookie, tag, web beacon, or analytics tool. It is a sophisticated computer software that enables Session Replay Providers to secretly and contemporaneously intercept, capture, read, observe, re-route, forward, redirect, and receive incoming electronic communications to Defendant's website.

6. The CEO of a major Session Replay Provider—while discussing the merger of his company with another Session Replay Provider—publicly exposed why companies like Defendant employ the use of Session Replay Code on their websites: "The combination of Clicktale and Contentsquare heralds an unprecedented goldmine of digital data that enables companies to interpret and predict the impact of any digital element—including user experience, content, price, reviews and product—on visitor behavior[.]"[1] This CEO further admitted that "this unique data can be used to activate custom digital experiences in the moment via an ecosystem of over 50

[1] *See Contentsquare Acquires Clicktale to Create the Definite Global Leader in Experience Analytics*, available at www.prnewswire.com/news-releases/contentsquare-acquires-clicktale-to-create-the-definitive-global-leader-in-experience-analytics-300878232.html (last accessed August 21, 2023).

martech partners. With a global community of customers and partners, we are accelerating the interpretation of human behavior online and shaping a future of addictive customer experiences."[2]

7. Unlike typical website analytics services that provide simple aggregate statistics, the Session Replay Code utilized by Defendant is intended to record and playback individual browsing sessions. The technology also permits companies like Defendant to view the interactions of visitors on their websites in real-time, including capturing partial text field submissions that users did not intend to send to Defendant (for example, by closing the browser before hitting "submit"), and certainly did not intend to send to third-party Session Replay Providers.

8. Spirit's conduct violates the California Penal Code § 631, Statutory Larceny, Cal. Pen. Code §§ 484, 496, Unfair Competition Law, Cal. Bus. & Prof. Code §§ 17200, *et seq.*, Maryland Wiretapping and Electronic Surveillance Act, Md. Code. Ann ("MWESA")., Cts. & Jud. Proc. § 10-401, Pennsylvania Wiretapping and Electronic Surveillance Control Act ("WESCA"), 18 Pa. C.S.A. § 5701, *et. seq*., and constitutes an invasion of the privacy rights of website visitors.

9. Plaintiffs bring this action individually and on behalf of a class of all natural persons in the states of California, Maryland, and Pennsylvania whose Website Communications were intercepted through Spirit's procurement and use of Session Replay Code embedded on www.spirit.com, as well as its subpages, and seeks all civil remedies provided under the causes of action, including but not limited to compensatory, statutory, and/or punitive damages, and attorneys' fees and costs.

PARTIES

10. Plaintiff Malinda S. Smidga is a citizen of the Commonwealth of Pennsylvania, and at all times relevant to this action, resided and was domiciled in Allegheny County, Pennsylvania.

---

[2] *Id.*

Plaintiff Smidga is a citizen of Pennsylvania and accessed www.spirit.com while in the Commonwealth of Pennsylvania.

11. Plaintiff Frances Curd is a citizen of the State of Maryland, and at all times relevant to this action, resided and was domiciled in Anne Arundel County, Maryland. Plaintiff Curd is a citizen of Maryland and accessed www.spirit.com while in the State of Maryland.

12. Plaintiff Kayla Mandeng is a citizen of the State of California, and at all times relevant to this action, resided and was domiciled in San Diego County, California. Plaintiff Mandeng is a citizen of California and accessed www.spirit.com while in the State of California.

13. Defendant Spirit Airlines, Inc. is a corporation organized under the laws of Delaware, and its principal place of business is in Miramar, Florida. Defendant is a citizen of Florida.

JURISDICTION AND VENUE

14. This Court has subject matter jurisdiction pursuant to 28 U.S.C. § 1332(d)(2)(A) because this case is a class action where the aggregate claims of all members of the proposed class are in excess of $5,000,000.00, exclusive of interest and costs, there are 100 or more members of the proposed class, and at least one member of the proposed class, including Plaintiffs, is a citizen of a state different than Defendant.

15. This Court has general jurisdiction over Defendant pursuant to Pa. C.S.A. § 5301. Specifically, this Court has general jurisdiction over Defendant because Defendant is an out-of-state corporation registered to do business under the laws of the Commonwealth of Pennsylvania since March 18, 1994. As part of registering to do business in the Commonwealth of Pennsylvania, Spirit Airlines "shall enjoy the same rights and privileges as a domestic entity and shall be subject to the same liabilities, restrictions, duties and penalties . . . imposed on domestic entities." Pa.

C.S.A. § 402(d). Among other things, Pennsylvania law is explicit that "qualification as a foreign entity under the laws of [the] Commonwealth" shall permit state courts to "exercise general personal jurisdiction" over a registered foreign corporation, just as they can over a domestic corporation. Pa. C.S.A. § 5301. Thus, by registering to do business in the Commonwealth of Pennsylvania and benefiting from the opportunity to do business in the Commonwealth of Pennsylvania, Defendant has consented to being subject to general jurisdiction in the Commonwealth of Pennsylvania.

16. In the alternative, this Court has specific personal jurisdiction over Defendant because a substantial part of the events and conduct giving rise to Plaintiffs' claims and harm occurred in the Commonwealth of Pennsylvania, the State of Maryland, and the State of California. The privacy violations complained of herein resulted from Defendant's purposeful and tortious acts directed towards citizens throughout these states. At all relevant times, Defendant knew that its practices would directly result in the collection of information from individuals located within California, Maryland, and Pennsylvania while those individuals browsed Defendant's website. Defendant chose to avail itself of the business opportunities of marketing, selling, and shipping their goods in California, Maryland, and Pennsylvania, and procuring the interception of real-time data from website visitors' sessions initiated by individuals while located in those places, and the claims alleged herein arise from those activities.

17. Spirit offers numerous flights to and from locations in Pennsylvania, including to and from Pittsburgh International Airport ("PIT"), the Philadelphia International Airport ("PHL"), and the Arnold Palmer Regional Airport ("LBE") in Latrobe, Pennsylvania. Through Spirit's Pennsylvania flight offerings, Spirit generates substantial revenue from its Pennsylvania contacts as it is PIT's fifth largest airline, carrying more than 10 percent of the airport's passengers and has

carried more than 2.5 million passengers at PIT since 2017.[3] Likewise, Spirit is the third-largest airline at PHL, serving 871,000 passengers at PHL between January and September 2021 alone.[4]

18. Spirit is continuously made aware that its website is being visited by people located in Pennsylvania, California, and Maryland, and that such website visitors are being wiretapped in violation of Pennsylvania, California, and Maryland statutory and common law. Additionally, Spirit directly engages in commerce in California and Maryland by offering flights to and from airports located in these states. Through its website, www.spirit.com, Spirit identifies six airports in California which it serves: Oakland, Los Angeles, San Diego, Burbank, Orange County and Sacramento, as well as Baltimore International Airport, which is located in Maryland.

19. Both desktop and mobile versions of Spirit's website allow a user to search for nearby airports, by providing the user's current location, as furnished by the location-determining tools of the device the user is using or by the user's IP address (*i.e.*, without requiring the user to manually input an address). Users' employment of automatic location services in this way means that Spirit is continuously made aware that its website is being visited by people located in California, Maryland, and Pennsylvania, and that such website visitors are being wiretapped in violation of California, Maryland, and Pennsylvania statutory and common law.

20. This Court has personal jurisdiction over Defendant because the wrongful conduct giving rise to this case occurred in, was directed to, and/or emanated from California, Maryland, and Pennsylvania. Defendant procured and embedded Session Replay Code, which it used to allow

[3] Evan Dougherty, *Spirit Airlines Celebrates 5 Years of Service at PIT*, Blue Sky News (May 23, 2022), https://blueskypit.com/2022/05/23/spirit-airlines-celebrates-5-years-of-service-at-pit/.
[4] Laura Smythe, *Spirit Airlines exec says there's 'still more opportunity' in Philadelphia following announcement of 7 new routes*, Philadelphia Business Journal (Dec. 8, 2021), https://www.bizjournals.com/philadelphia/news/2021/12/08/more-opportunity-spirit-airlines-phl-executive.html.

Session Replay Providers to collect data directly from website visitors in each of these three states, violating statutory and common law.

21. Furthermore, Defendant actively uses the data collected by Session Replay Providers in all fifty states to specifically target citizens of each state with marketing and advertising content which results in an increased profit to Defendant at a significant cost to Plaintiffs and Class Members in the form of loss of privacy.

22. Defendant's decision to place or procure the placement of Session Reply Code to collect the data of citizens of Pennsylvania, Maryland, and California, is by deliberate and intentional design.

23. Though Plaintiffs and Class Members do not currently have the ability to do so, if a user chose to deny Defendant permission to collect the user data or employ the Session Replay Code on their computers and/or mobile devices, Defendant's profits would be reduced because they would be unable to track Plaintiffs, gather information about them, or push ads which result in profit.

24. Defendant's deliberate gathering of the data is intentionally targeted toward, and constitutes purposeful activity directed at the citizens, residents, and visitors of Pennsylvania, Maryland, and California, including Plaintiffs and the Classes.

25. Defendant's deliberate placement of Session Replay Code on the computers and mobile devices of unwitting browsers in the United States results in a trespass to chattels—*i.e.*, the computers and/or mobile devices and/or the data contained therein; and a conversion of chattels—*i.e.*, the computers and/or mobile devices and/or the data contained therein. Given the placement of the Session Replay Code on Defendant's website to intercept data from website browsers

nationwide, and the use of such intercepted data for specific targeting advertisements and profit, Defendant could not be surprised to be hailed into court in Pennsylvania, Maryland, or California.

26. Pursuant to 28 U.S.C. § 1391, this Court is the proper venue for this action because a substantial part of the events, omissions, and acts giving rise to the claims herein occurred in this District. Further, Pennsylvania has the greatest material interest in protecting the citizens in the Commonwealth of Pennsylvania and enforcing WESCA given that the interception of Plaintiff's and Class Member's communications occurred from within the borders of the Commonwealth.

ARTICLE III STANDING

27. Plaintiffs all have Article III standing to pursue their claims. As an initial matter, the statutory claims pleaded by Plaintiffs below codify substantive rights to privacy. *See e.g., In re Facebook, Inc. Internet Tracking Litigation*, 956 F.3d 589, 598 (9th Cir. 2020) ("[T]he legislative history and statutory text demonstrate that Congress and the California legislature intended to protect these historical privacy rights when they passed the Wiretap Act, SCA, and CIPA."); *Campbell v. Facebook, Inc*., 951 F.3d 1106, 1117–18 (9th Cir. 2019) ("[T]he intrusion itself makes defendant subject to liability…wiretapping is actionable…a wiretapping plaintiff need not allege any further harm to have standing.").

28. Plaintiffs' claims arise under the core substantive provisions of state wiretapping statutes, and state privacy, theft, trespass to chattels, conversion to chattels, and unfair competition statutes, and as such, confer standing.

29. The core provisions of the statutes pled below are targeted at the substantive intrusion that occurs when private communications are intercepted by someone who does not have the right to access them, rather than merely setting out a procedure for handling data.

30. Importantly, the state wiretapping statutes are content-neutral laws of general applicability, whose primary purpose is to protect the privacy of wire, oral, and electronic

communications by virtue of the fact that they were illegally intercepted *i.e.*, "by virtue of the source rather than the subject matter." *Bartnicki v. Vopper*, 532 U.S. 514, 517 (2001).

31. In the counts pleaded herein, Plaintiffs plead statutes that codify a content-specific extension of the substantive right to privacy: these statutes protect Plaintiffs' substantive privacy interest in their Website Communications. Every interception and disclosure of Plaintiffs' Website Communications offends the interests that these statutes protect and constitutes a concrete injury.

32. Plaintiffs allege that Defendant procured Session Replay Providers to collect their data without consent and have violated the concrete privacy interests that state wiretapping statutes and state privacy, theft, and unfair competition statutes, as well as the common law torts of invasion of privacy and intrusion upon seclusion, protect.

33. Moreover, Plaintiffs allege that Defendant's procurement of Session Replay Providers to surreptitiously and instantaneously record every Website Communication is highly offensive and Plaintiffs have suffered concrete injury from Defendant's conduct.

34. Plaintiffs allege specific facts demonstrating that the only reason Defendant has access to the aggregated data of Plaintiffs and Class Members is the illegal collection and storage of information from Plaintiffs' Website Communications by third parties without consent. These allegations constitute concrete injuries under the substantive rights the statutes—and the common law torts—protect.

35. That the information collected by third parties procured by Defendant was private Website Communications and was later used by Defendant, and by third parties, to facilitate its own products and services for financial gains also constitutes a concrete injury to Plaintiffs and Class Members.

36. Plaintiffs also allege that the third parties hired by Defendant aggregate and store Plaintiffs' and Class Members' data under unique identifiers. Thus, even if the individual data points gathered are anonymous by themselves, when aggregated, Session Replay Providers and Defendant use them to uniquely identify each user, creating a "fingerprint" for each individual, which supports a showing of concrete harm.

37. Defendant has profited from Plaintiffs' Website Communications and has profited from the collection of Plaintiffs' data. All Class Members seek individual damages for these concrete injuries.

38. Plaintiffs also allege that their Website Communications have monetary value for which they were not paid. Because statutes pleaded by Plaintiffs (UCL, for example) afford them the right to prevent Defendant and its Session Replay Providers from utilizing their data for profit, they have a property interest in their data and have suffered an injury-in-fact by Defendant's collection, storage, use and sharing of Plaintiffs' private browsing information.

39. In addition, Plaintiffs have Article III standing to pursue injunctive relief. To establish standing for prospective injunctive relief, a plaintiff must demonstrate "continuing, present adverse effects." *City of Los Angeles v. Lyons,* 461 U.S. 95, 102 (1983).

40. Plaintiffs desire to continue to use Defendant's website but Defendant's conduct is ongoing; Defendant continues to unlawfully cause the interception of Plaintffs' and Class Members' Website Communications any time they visit Defendant's website with Session Replay Code enabled without their consent. Defendant's conduct has not stopped, and it will continue to allow third parties to collect users' private browsing data for its own use without Plaintiffs' and Class Members' express consent.

41. Plaintiffs have pled sufficient facts alleging concrete injuries for common law torts of invasion of privacy and intrusion upon seclusion, state wiretapping statutes, and state privacy, theft and unfair competition statutes.

FACTUAL ALLEGATIONS

A. Website User and Usage Data Have Immense Economic Value.

42. The "world's most valuable resource is no longer oil, but data."[5]

43. In 2022, Business News Daily reported that some businesses collect personal data (*i.e.*, gender, web browser cookies, IP addresses, and device IDs), engagement data (*i.e.*, how consumers interact with a business's website, applications, and emails), behavioral data (*i.e.*, customers' purchase histories and product usage information), and attitudinal data (*i.e.*, data on consumer satisfaction) from consumers.[6] This information is valuable to companies because they can use this data to improve customer experiences, refine their marketing strategies, capture data to sell it, and even to secure more sensitive consumer data.[7]

44. In a consumer-driven world, the ability to capture and use customer data to shape products, solutions, and the buying experience is critically important to a business's success. Research shows that organizations who "leverage customer behavior insights outperform peers by 85 percent in sales growth and more than 25 percent in gross margin."[8]

---

[5] *The world's most valuable resource is no longer oil, but data*, The Economist (May 6, 2017), https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data.

[6] Max Freedman, *How Businesses Are Collecting Data (And What They're Doing With It)*, Business News Daily (Aug. 5, 2022), https://www.businessnewsdaily.com/10625-businesses-collecting-data.html.

[7] *Id.*

[8] Brad Brown, Kumar Kanagasabai, Prashant Pant & Goncalo Serpa Pinto, *Capturing value from your customer data*, McKinsey (Mar. 15, 2017), https://www.mckinsey.com/business-functions/quantumblack/our-insights/capturing-value-from-your-customer-data.

45. In 2013, the Organization for Economic Cooperation and Development ("OECD") even published a paper entitled "Exploring the Economics of Personal Data: A Survey of Methodologies for Measuring Monetary Value."[9] In this paper, the OECD measured prices demanded by companies concerning user data derived from "various online data warehouses."[10]

46. OECD indicated that "[a]t the time of writing, the following elements of personal data were available for various prices: USD 0.50 cents for an address, USD 2 [i.e. $2] for a date of birth, USD 8 for a social security number (government ID number), USD 3 for a driver's license number and USD 35 for a military record. A combination of address, date of birth, social security number, credit record and military is estimated to cost USD 55."[11]

B. Website Users Have a Reasonable Expectation of Privacy in Their Interactions with Websites.

47. Consumers are skeptical and are wary about their data being collected. A report released by KPMG shows that "a full 86% of the respondents said they feel a growing concern about data privacy, while 78% expressed fears about the amount of data being collected."[12]

48. Another recent paper also indicates that most website visitors will assume their detailed interactions with a website will only be used by the website and not be shared with a party

[9] Exploring the Economics of Personal Data: A Survey of Methodologies for Measuring Monetary Value, OECD Digital Economy Papers, NO. 220 (Apr. 2, 2013), https://www.oecdilibrary.org/docserver/5k486qtxldmq-en.pdf.
[10] *Id.* at 25.
[11] *Id.*
[12] Lance Whitney, *Data privacy is a growing concern for more consumers*, TechRepublic (Aug. 17, 2021), https://www.techrepublic.com/article/data-privacy-is-a-growing-concern-for-more-consumers/.

they know nothing about.[13] As such, website visitors reasonably expect that their interactions with a website should not be released to third parties unless explicitly stated.[14]

49. Privacy polls and studies show that a majority of Americans consider one of the most important privacy rights to be the need for an individual's affirmative consent before a company collects and shares its customers' data.

50. A recent study by Consumer Reports shows that 92% of Americans believe that internet companies and websites should be required to obtain consent before selling or sharing consumers' data, and the same percentage believe internet companies and websites should be required to provide consumers with a complete list of the data that has been collected about them.[15]

51. Moreover, according to a study by Pew Research Center, a majority of Americans, approximately 79%, are concerned about how data is collected about them by companies.[16]

52. Users act consistently with their expectation of privacy. Following a new rollout of the iPhone operating software—which asks users for clear, affirmative consent before allowing companies to track users—85 percent of worldwide users and 94 percent of U.S. users chose not to allow such tracking.[17]

---

[13] *CUJO AI Recent Survey Reveals U.S. Internet Users Expectations and Concerns Towards Privacy and Online Tracking*, CUJO (May 26, 2020), https://www.prnewswire.com/news-releases/cujo-ai-recent-survey-reveals-us-internet-users-expectations-and-concerns-towards-privacy-and-online-tracking-301064970.html.

[14] Frances S. Grodzinsky, Keith W. Miller & Marty J. Wolf, *Session Replay Scripts: A Privacy Analysis*, The Information Society, 38:4, 257, 258 (2022).

[15] *Consumers Less Confident About Healthcare, Data Privacy, and Car Safety, New Survey Finds*, Consumer Reports (May 11, 2017), https://www.consumerreports.org/consumer-reports/consumers-less-confident-about-healthcare-data-privacy-and-car-safety/.

[16] *Americans and Privacy: Concerned, Confused, and Feeling Lack of Control Over Their Personal Information*, Pew Research Center, (Nov. 15, 2019), https://www.pewresearch.org/internet/2019/11/15/americans-and-privacy-concerned-Confused-and-feeling-lack-of-control-over-their-personal-information/.

[17] Margaret Taylor, *How Apple screwed Facebook*, Wired, (May 19, 2021), https://www.wired.co.uk/article/apple-ios14-facebook.

C. How Session Replay Code Works.

53. Session Replay Code, such as that which Defendant implements on its website, enables website operators to intercept, capture, read, observe, re-route, forward, redirect, record, save, analyze and replay website visitors' interactions with a given website. The clandestinely deployed code provides online marketers and website designers with detailed insights into user behavior by intercepting and recording website visitors "as they click, scroll, type or navigate across different web pages."[18]

54. While Session Replay Code is utilized by websites for some legitimate purposes, it goes well beyond normal website analytics when it comes to collecting the actual contents of communications between website visitors and websites. Unlike other online advertising tools, Session Replay Code allows a website to capture and record nearly every action a website visitor takes while visiting the website, including actions that reveal the visitor's personal or private sensitive data, sometimes even when the visitor does not intend to submit the data to the website operator, has enabled private browsing such as "Incognito Mode" with the intention of masking their activities and information, or has not finished submitting the data to the website operator.[19] As a result, website visitors "aren't just sharing data with the [web]site they're on . . . but also with an analytics service that may be watching over their shoulder."[20]

---

[18] Erin Gilliam Haije, *[Updated] Are Session Recording Tools a Risk to Internet Privacy?*, Mopinion (Mar. 7, 2018), https://mopinion.com/are-session-recording-tools-a-risk-to-internet-privacy/.

[19] *Id.*

[20] Eric Ravenscraft, *Almost Every Website You Visit Records Exactly How Your Mouse Moves*, Medium (Feb. 5, 2020), https://onezero.medium.com/almost-every-website-you-visit-records-exactly-how-your-mouse-moves-4134cb1cc7a0.

55. The Session Replay Code utilized by Defendant works by inserting computer code into the various event handling routines that web browsers use to receive input from users, thus intercepting the occurrence of communications initiated by the actions the user takes.[21] Simply put, when a user interacts with the website, they transmit substantive information via electronic communications in the form of instructions to Defendant's computer servers utilized to operate the website. These commands are sent as messages instructing the website host, like Defendant, what content was being viewed, clicked on, requested and/or inputted by the user.

56. When Defendant's website delivers Session Replay Code to a user's browser, the user's browser will follow the code's instructions by contemporaneously sending duplicated responsive messages of the user's communications, in the form of "Event" data, to a designated third-party Session Replay Provider server. Upon information and belief, the servers receiving the event data are exclusively controlled by the third-party entity that wrote the Session Replay Code, rather than the owner of the website where the code is installed.

57. The types of communications captured by the Session Replay Code utilized by Defendant encompass virtually every user action, including all mouse movements, clicks, scrolls, zooms, window resizes, keystrokes, text entries, and numerous other forms of a user's navigation and interaction through Defendant's website. To permit a reconstruction of a user's visit accurately, the Session Replay Code is capable of capturing these events at hyper-frequent intervals, often just milliseconds apart. Events are accumulated and transmitted in blocks

---

[21] These communications occur through the Hypertext Transfer Protocol ("HTTP"). HTTP works as a request-response protocol between a user and a server as the user navigates a website. A GET request is used to request data from a specified source. A POST request is used to send data to a server. *See HTTP Request Methods,* located at https://www.w3schools.com/tags/ref_httpmethods.asp (last visited August 21, 2023).

periodically throughout the user's website session, rather than after the user's visit to the website is completely finished.

58. Unless specifically masked through configurations chosen by the website owner, visible contents of Website Communications are also transmitted to the Session Replay Provider.

59. Once the events from a user session have been recorded by a Session Replay Code, Defendant's procured Session Replay Providers (whose existence and identity is unknown to Plaintiffs and the Class Members) store the raw data to be interpreted and reproduced so that Defendant can view a visual reenactment of the user's visit through the Session Replay Provider's proprietary service platform, usually in the form of a video, meaning that "[u]nlike typical analytics services that provide aggregate statistics, these scripts are intended for the recording and playback of individual browsing sessions."[22] Moreover, the raw event data is neither readily accessible or interpretable by Defendant itself; instead the raw event data is in the custody and control of the Session Replay provider, who has the ability to interpret and replay the data.

60. The extent and detail of the data collected by the Session Replay Providers for users of the technology, such as Defendant, far exceeds the stated purpose and Plaintiffs' and the Class Members' reasonable expectations when visiting websites like those of Defendant. Indeed, in a patent dispute, a highly utilized Session Replay Provider openly admitted that this type of technology is utilized by companies like Defendant to make a profit: "[the] software computes billions of touch and mouse movements and transforms this knowledge into profitable actions that

---

[22] Steven Englehardt, *No boundaries: Exfiltration of personal data by session-replay scripts*, Freedom to Tinker (Nov. 15, 2017), https://freedom-to-tinker.com/2017/11/15/no-boundaries-exfiltration-of-personal-data-by-session-replay-scripts/.

increase engagement, reduce operational costs, and maximize conversion rates (i.e., the percentage of users who take desired actions on a website, such as purchasing a product offered for sale)."[23]

61. Further, because most Session Replay Codes will by default indiscriminately capture the maximum range of user-initiated events and content displayed by the website, researchers have found that a variety of highly sensitive information can be captured in event responses from website visitors, including medical conditions, credit card details, and other personal information displayed or entered on webpages. Upon information and belief, the Session Replay Code utilized by Defendant captures data including such highly sensitive information.

62. Most alarming, the Session Replay Code captures data that the user did not even intentionally transmit to a website during a visit, and then makes that data available to Defendant when they access the session replay through the Session Replay Provider. For example, if a user writes information into a text form field, but then chooses not to click a "submit" or "enter" button on the website, the Session Replay Code will nevertheless cause the non-submitted text to be sent to the designated event-response-receiving Session Replay Provider's server before the user deletes the text or leaves the page. This information will then be viewable to Defendant when accessing the session replay through the Session Replay Provider.

63. Session Replay Code does not necessarily anonymize user sessions, either.

64. First, if a user's entry of personally identifying information is captured in an event response, that data will become known and visible to both the Session Replay Provider and the website owner.

[23] *Content Square SAS v. Quantum Metric, Inc.,* Case No. 1:20-cv-00832-LPS, Compl. at ¶ 8 [DE 1] (D. Del. Jun. 22, 2020).

65. Second, if a website displays user account information to a logged-in user, that content may be captured by Session Replay Code.

66. Third, some Session Replay Providers, including those utilized by Defendant, explicitly offer website owners functionality that permits linking a session to an identified user, who may be personally identified if the website owner has associated the user with an email address or username.[24]

67. Session Replay Providers often create "fingerprints" that are unique to a particular user's combination of computer and browser settings, screen configuration, and other detectable information. The resulting fingerprint, which is often unique to a user and rarely changes, are collected across all sites that the Session Replay Provider monitors.

68. When a user eventually identifies themselves to one of these websites (such as by filling in a form), the provider can then associate the fingerprint with the user identity and can then back-reference all of that user's other web browsing across other websites previously visited, including on websites where the user had intended to remain anonymous—even if the user explicitly indicated that they would like to remain anonymous by enabling private browsing.

69. In addition to the privacy invasions caused by the diversion of user communications with websites to third-party Session Replay Providers, Session Replay Code also exposes website visitors to identity theft, online scams, and other privacy threats.[25] Indeed, "[t]he more copies of

---

[24] *Id.*; *see also FS.identify – Identifying users*, FullStory, https://help.fullstory.com/hc/en-us/articles/360020828113, (last visited August 8, 2023); *FAQ - Are you able to follow user sessions across devices?*, Quantum Metric, https://www.quantummetric.com/faq/, (last visited August 21, 2023); *How does Mouseflow detect new and returning visitors?*, Mouseflow, https://help.mouseflow.com/en/articles/4361083-how-does-mouseflow-detect-new-and-returning-visitors (last visited August 21, 2023).

[25] Juha Sarrinen, *Session Replay is a Major Threat to Privacy on the Web*, itnews (Nov. 16, 2017), https://www.itnews.com.au/news/session-replay-is-a-major-threat-to-privacy-on-the-web-477720.

sensitive information that exist, the broader the attack surface, and when data is being collected [… .] it may not be stored properly or have standard protections" increasing "the overall risk that data will someday publicly leak or be breached."[26] Moreover, users are deprived of their capacity to consent to the additional storage of their communications and personal information by a third-party.

70. The privacy concerns arising from Session Replay Code are not theoretical or imagined. The CEO and founder of LOKKER, a provider of data privacy and compliance solutions has said "[consumers] should be concerned" about the use of Session Replay Code because "they won't know these tools are operating 'behind the scenes' of their site visit" and "even if the company disclosed that they are using these tools, consumers wouldn't likely be able to opt-out and still use the site."[27] True to this statement, Defendant's website offers no opportunity to opt-out of its use of Session Replay Code, including if a user utilizes a private browsing mode on their browser.

71. Indeed, the news is replete with examples of the dangers of Session Replay Code. For example, in 2019, the App Analyst, a mobile expert who writes about his analyses of popular apps, found that Air Canada's iPhone app wasn't properly masking the session replays they were

---

[26] Lily Hay Newman, *Covert 'Replay Sessions' Have Been harvesting Passwords by Mistake*, WIRED (Feb. 26, 2018), https://www.wired.com/story/covert-replay-sessions-harvesting-passwords/.

[27] Mark Huffner, *Is 'session replay software' a privacy threat or just improving your web experience*, Consumer Affairs (Oct. 25, 2022), https://www.consumeraffairs.com/news/is-session-replay-software-a-privacy-threat-or-just-improving-your-web-experience-102522.html.

sent, exposing unencrypted credit card data and password information.[28] This discovery was made just weeks after Air Canada said its app had a data breach, exposing 20,000 profiles.[29]

72. Further, multiple companies have removed Session Replay Code from their websites after it was discovered the Session Replay Code captured highly sensitive information. For instance, in 2017, Walgreens stopped sharing data with a Session Replay Provider after it was discovered that the Session Replay Provider gained access to website visitors' sensitive information.[30] Indeed, despite Walgreens' extensive use of manual redactions for displayed and inputted data, the Session Replay Provider still gained access to full names of website visitors, their medical conditions, and their prescriptions.[31]

73. Following the Walgreens incident, Bonobos, a men's clothing retailer, announced that it was eliminating data sharing with a Session Replay Provider after it was discovered that the Session Replay Provider captured credit card details, including the cardholder's name and billing address, and the card's number, expiration, and security code from the Bonobos' website.[32]

74. Recognizing the privacy concerns posed by Session Replay Code, in 2019 Apple required app developers to remove or properly disclose the use of analytics code that allow app developers to record how a user interacts with their iPhone apps or face immediate removal from

---

[28] Zach Whittaker, *Many Popular iPhone Apps Secretly Record Your Screen Without Asking*, TechCrunch (Feb. 6, 2019), https://techcrunch.com/2019/02/06/iphone-session-replay-screenshots/.

[29] *Id.*

[30] Nitasha Tiku, *The Dark Side of 'Replay Sessions' That Record Your Every Move Online*, WIRED (Nov. 16, 2017), https://www.wired.com/story/the-dark-side-of-replay-sessions-that-record-your-every-move-online/.

[31] Englehardt, *supra* note 22.

[32] Tiku, *supra* note 30.

the app store.[33] In announcing this decision, Apple stated: "Protecting user privacy is paramount in the Apple ecosystem. Our App Store Review Guidelines require that apps request explicit user consent and provide a clear visual indication when recording, logging, or otherwise making a record of user activity."[34]

75. Consistent with Apple's concerns, countless articles have been written about the privacy implications of recording user interactions during a visit to a website, including the following examples:

(a) ***The Dark Side of 'Replay Sessions' That Record Your Every Move Online***, located at https://www.wired.com/story/the-dark-side-of-replay-sessions-that-record-your-every-move-online/ (last visited August 21, 2023);

(b) ***Session-Replay Scripts Disrupt Online Privacy in a Big Way***, located at https://www.techrepublic.com/article/session-replay-scripts-are-disrupting-online-privacy-in-a-big-way/ (last visited August 21, 2023);

(c) ***Are Session Recording Tools a Risk to Internet Privacy?***, located at https://mopinion.com/are-session-recording-tools-a-risk-to-internet-privacy/ (last visited August 21, 2023);

(d) ***Session Replay is a Major Threat to Privacy on the Web***, located at https://www.itnews.com.au/news/session-replay-is-a-major-threat-to-privacy-on-the-web-477720 (last visited August 21, 2023);

---

[33] Zack Whittaker, *Apple Tells App Developers to Disclose or Remove Screen Recording Code*, TechCrunch (Feb. 7, 2019), https://techcrunch.com/2019/02/07/apple-glassbox-apps/.

[34] *Id.*

(e) ***Session Replay Scripts Could be Leaking Sensitive Data***, located at https://medium.com/searchencrypt/session-replay-scripts-could-be-leaking-sensitive-data-5433364b2161 (last visited August 21, 2023);

(f) ***Website Owners can Monitor Your Every Scroll and Click***, located at https://www.digitalinformationworld.com/2020/02/top-brands-and-websites-can-monitor-your-every-scroll-and-click.html (last visited August 21, 2023); and

(g) ***Sites Using Session Replay Scripts Leak Sensitive User Data***, located at https://www.helpnetsecurity.com/2017/11/20/session-replay-data-leak (last visited August 21, 2023).

D. Spirit Secretly Wiretaps and Procures Session Reply Providers to Wiretap its Website Visitors' Electronic Communications.

76. Spirit operates the website www.spirit.com, as well as all of its subpages. Spirit is an airline whose planes serve more than ninety destinations across the country.

77. Spirit's website allows website visitors to search for flights. However, Spirit's website includes many other links and features including sections for "Investor Relations," "Careers," and the "Spirit Charitable Foundation."[35] Spirit's website also provides information about the Free Spirit ® World Elite Mastercard® (including a button that links to a page where one can apply for the card).[36] Finally, Spirit's website has modules for booking hotels, cars, and even cruises—*i.e.*, travel-related services separate and distinct from air transportation.[37]

78. However, unbeknownst to the millions of individuals browsing Spirit's website, Spirit intentionally procures and embeds various Session Replay Codes from Session Replay

35 *See* https://www.spirit.com/ (last visited August 21, 2023).
36 *Id.*
37 *Id.*

Providers on its website to track and analyze website user interactions with www.spirit.com and its subpages.

79. One such Session Replay Provider that Spirit procures is FullStory.

80. Each of these Session Replay Codes used by Defendant provides detailed information about website user sessions, interactions, and engagement, with the capacity to break down users by device type, location, and other dimensions.[38]

81. FullStory is the owner and operator of a Session Replay Code titled FullStory Script, which records all website visitor actions, including information typed by the website users while on the website. Such information can include names, emails, phone numbers, addresses, social security numbers, date of birth, and more. Research by the Princeton University Center for Information Technology Policy found that "text typed into forms is collected before the user submits the form, and precise mouse movements are saved, all without any visual indication to the user."[39]

82. As a user interacts with any website with the embedded FullStory Script, "each click, tap, URL visit, and every other interaction is sent in tiny little packets to that existing session at FullStory servers."[40] This includes button clicks, mouse movements, scrolling, resizing, touches

---

[38] *See* Jono Alderson, *An Introduction to Microsoft Clarity*, Yoast, https://yoast.com/introduction-microsoft-clarity/#h-what-is-microsoft-clarity, (last visited Sep. 8, 2022); *Search for Recordings by a User's IP Address, Location, and Other Identifiers*, Mouseflow, https://help.mouseflow.com/en/articles/5882714-search-for-recordings-by-a-user-s-ip-address-location-and-other-identifiers, (last visited August 21, 2023);); *FAQ - Are you able to follow user sessions across devices?*, Quantum Metric, https://www.quantummetric.com/faq/, (last visited August 21, 2023).

[39] Englehardt, *supra* note 22.

[40] *Id.*

(for mobile browsers), key presses, page navigation, changes to visual elements in the browsers, network requests, and more.[41]

83. As such, the FullStory Script collects highly personal information and substantive communications that can be linked directly to a website user's identity as it monitors, records, and collects a website user's every move. And like other Session Replay Codes, the information collected and recorded by the FullStory Script can then be used to play back a user's journey through a website, showing how they interacted with site navigation, calls to action, search features, and other on-page elements. Put differently, the information the FullStory Script captures can be translated into a simulation video of how a user interacts with a website.

84. Finally, the FullStory Script enables collecting website visitors' IP addresses and geolocation data in a visible and searchable format for websites such as Spirit. Indeed, the FullStory Script uses IP addresses "to surface geolocation data" and in turn, "[t]his geolocation data allows users to segment for sessions by country, state, or city."[42] Put differently, by capturing IP address information, the FullStory Script enables websites, such as Spirit, to search recorded website user sessions by specific locations that is "fairly accurate" at the country and state level, and less so at the city level.[43]

85. Importantly, the FullStory Script captures IP addresses by default and the FullStory Script requires websites such as Spirit to manually toggle "Discard user IP addresses" to "off" in the FullStory Script's data capture and privacy settings if they do not want the FullStory Script to

---

[41] *How does FullStory capture data to recreate my users' experience?*, FullStory, https://help.fullstory.com/hc/en-us/articles/360032975773-How-does-FullStory-capture-data-to-recreate-my-users-experience-, (last visited Nov. 21, 2022) (hereinafter "FullStory Data Capture").

[42] *IP Address & Geolocation*, FullStory, https://help.fullstory.com/hc/en-us/articles/360045926353-IP-Address-Geolocation (last visited August 21, 2023).

[43] *Id.*

maintain IP addresses in a readily visible and searchable manner.[44] And even if a website chooses to discard user IP addresses, this does not stop the FullStory Script from collecting and using the collect IP addresses to obtain other location data such as country or state.[45] Nor is this feature retroactive. If the FullStory Script has already provided IP addresses to clients, the IP addresses will remain searchable to clients until the client exceeds their "product analytics retention period and have been deleted."[46]

86. Given the breadth of information the FullStory Script collects, including a website user's IP address and geolocation data, it is inevitable that Spirit knows it is capturing, collecting, and recording the Website Communications of Pennsylvania, Maryland, and California residents.

87. Spirit's procurement and use of FullStory's Session Replay Code, and procurement and use of other Session Replay Codes through various Session Replay Providers, is a wiretap in violation of Pennsylvania, Maryland, and California statutory and common law. Indeed, once a website installs the FullStory Script, that code acts as a secret wiretap that sends users' Website Communications to FullStory in real time, instantly reporting every keystroke, movement, click, and/or moment of inactivity to the FullStory server.

E. Plaintiffs' and Class Members' Experience.

Plaintiff Smidga

88. Plaintiff Smidga has visited www.spirit.com and certain of its subpages on her computer while in Pennsylvania in the summer of 2021 to search for flights for her and her son.

[44] *Id.*
[45] *Id.*
[46] *Id.*

89. While visiting Spirit's website, Plaintiff Smidga fell victim to Defendant's unlawful monitoring, recording, and collection of Plaintiff Smidga's Website Communications with www.spirit.com prior to the filing of this action.

90. Unknown to Plaintiff Smidga, Spirit procures and embeds Session Replay Code on its website. In particular, the FullStory Script was operative on Spirit's website and subpages during Plaintiff Smidga's visits to Spirit's website.

91. During the visit by Plaintiff Smidga to www.spirit.com and its subpages, Plaintiff Smidga browsed for flight options to and from the Pittsburgh and Latrobe airports. Plaintiff Smidga communicated with Spirit's website by using her mouse to hover and click on certain flight options.

92. Even though Plaintiff Smidga did not end up purchasing any flights on her visit to Spirit's website, the Session Replay Code nevertheless instantaneously captured her Website Communications throughout her visit. Indeed, through Defendant's procurement of Session Replay Code, Plaintiff Smidga's Website Communications were automatically and secretly intercepted by using Defendant's website.

93. During Plaintiff Smidga's visit to Defendant's website, Plaintiff Smidga, through her computer, transmitted electronic communications in the form of instructions to Defendant's computer servers utilized to operate the website. The commands were sent as messages instructing Defendant what content was being viewed, clicked on, requested and/or inputted by Plaintiff Smidga. The communications sent by Plaintiff Smidga to Defendant's servers included, but were not limited to, the following actions taken by Plaintiff Smidga while on the website: mouse clicks and movements, keystrokes, search terms, substantive information inputted by Plaintiff Smidga, pages and content viewed by Plaintiff Smidga, scroll movement, and copy and paste actions.

94. Defendant responded to Plaintiff Smidga's electronic communications by supplying—through its website—the information requested by Plaintiff Smidga.

95. Plaintiff Smidga reasonably expected that her visit to Spirit's website would be private and that Defendant would not have procured a third party that was tracking, recording, and/or watching Plaintiff Smidga as she browsed, interacted with the website, and searched for products, particularly because Plaintiff Smidga was not presented with any type of pop-up disclosure, consent form, or privacy policy alerting Plaintiff Smidga that her visit to the website were being recorded by Defendant through a third party.

96. Defendant's data collection is highly offensive, and Plaintiff Smidga has suffered concrete injury from Defendant's vast collection, aggregation and use of Plaintiff Smidga's personal browsing histories without consent.

Plaintiff Curd

97. While in Maryland, Plaintiff Curd visited www.spirit.com and certain of its subpages on her computer in February and March 2022. She browsed for flight options and communicated with Spirit's website by using her mouse to hover and click on certain flight options and typing search words into the search bar.

98. Even though Plaintiff Curd did not end up purchasing any flights on her visits to Defendant's website, the Session Replay Code nevertheless instantaneously captured her Website Communications throughout her visit. Indeed, through Defendant's procurement of Session Replay Code, Plaintiff Curd's Website Communications were automatically and secretly intercepted by using Defendant's website.

99. During Plaintiff Curd's visit to Defendant's website, Plaintiff Curd, through her computer, transmitted electronic communications in the form of instructions to Defendant's

computer servers utilized to operate the website. The commands were sent as messages instructing Defendant what content was being viewed, clicked on, requested and/or inputted by Plaintiff Curd. The communications sent by Plaintiff Curd to Defendant's servers included, but were not limited to, the following actions taken by Plaintiff Curd while on the website: mouse clicks and movements, keystrokes, search terms, substantive information inputted by Plaintiff Curd, pages and content viewed by Plaintiff Curd, scroll movement, and copy and paste actions.

100. Defendant responded to Plaintiff Curd's electronic communications by supplying—through its website—the information requested by Plaintiff Curd.

101. Plaintiff Curd reasonably expected that her visit to Defendant's website would be private and that Defendant would not have procured a third party that was tracking, recording, and/or watching Plaintiff Curd as she browsed, interacted with the website, and searched for products, particularly because Plaintiff Curd was not presented with any type of pop-up disclosure, consent form, or privacy policy alerting Plaintiff Curd that her visit to the website was being recorded by Defendant through a third party.

102. Defendant's data collection is highly offensive, and Plaintiff Curd has suffered concrete injury from Defendant's vast collection, aggregation and use of Plaintiff Curd's personal browsing histories without consent.

Plaintiff Mandeng

103. While in California, Plaintiff Mandeng visited www.spirit.com on her computers and/or mobile devices.

104. Specifically, in September, 2022, Plaintiff Mandeng browsed available flights for her and her four (4) children on www.spirit.com and purchased tickets.

105. During Plaintiff Mandeng's visits to Defendant's website, Plaintiff Mandeng,

through her computer and/or mobile device, transmitted electronic communications in the form of instructions to Defendant's computer servers utilized to operate the website. The commands were sent as messages instructing Defendant what content was being viewed, clicked on, requested and/or inputted by Plaintiff Mandeng. The communications sent by Plaintiff Mandeng to Defendant's servers included, but were not limited to, the following actions taken by Plaintiff Mandeng while on the website: mouse clicks and movements, keystrokes, search terms, substantive information inputted by Plaintiff Mandeng, pages and content viewed by Plaintiff Mandeng, scroll movement, and copy and paste actions. During this process, Plaintiff Mandeng input the names, addresses, and ages of herself and her four (4) children, the departure and arrival locations for her potential trip, and her credit card and billing information.

106. Defendant responded to Plaintiff Mandeng's electronic communications by supplying—through its website—the information requested by Plaintiff Mandeng.

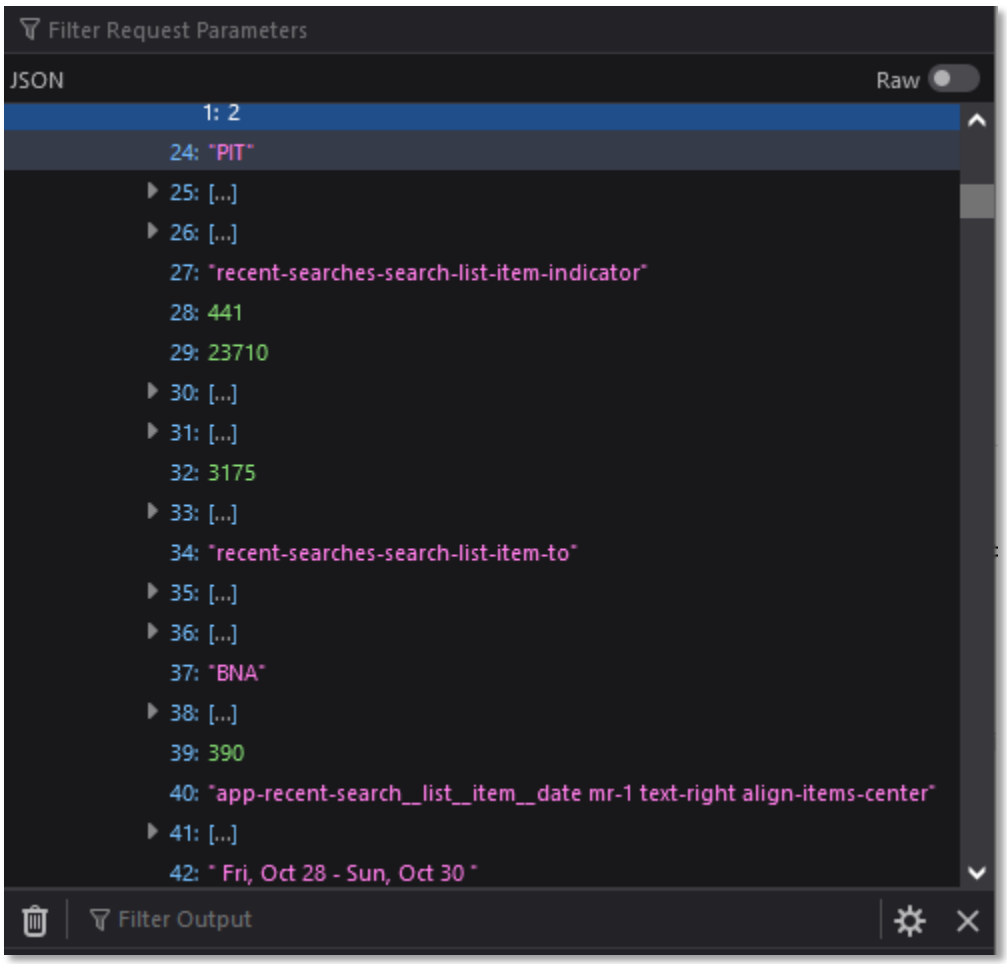
107. Plaintiff Mandeng reasonably expected that her visit to Defendant's website would be private and that Defendant would not have procured a third party that was tracking, recording, and/or watching Plaintiff Mandeng as she browsed, interacted with the website, and searched for products, particularly because Plaintiff Mandeng was not presented with any type of pop-up disclosure, consent form, or privacy policy alerting Plaintiff Mandeng that her visit to the website was being recorded by Defendant through a third party.

108. Defendant's data collection is highly offensive, and Plaintiff Mandeng has suffered concrete injury from Defendant's vast collection, aggregation and use of Plaintiff Mandeng's personal browsing histories without consent.

Plaintiffs' Experiences on Defendant's website

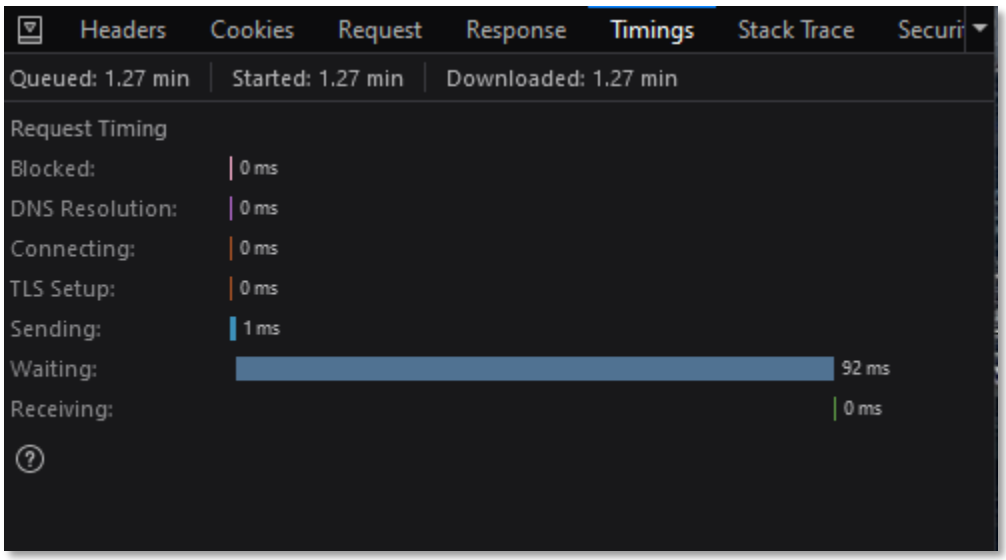
109. Further, without their consent, Spirit procured Session Replay Providers to obtain certain information about Plaintiffs' devices and browsers and create unique IDs and profiles for each of them.

110. For example, when visiting www.spirit.com and its subpages, if a website user searches for flights, that information is captured by the Session Replay Codes embedded on the website:



Depicting information sent to one of the Service Replay Providers—FullStory—through a Service Replay Code—FullStory Script—after entering looking for flights from Pittsburgh, PA (PIT) to Nashville, TN (BNA) on October 28 and returning October 30 on www.spirit.com.

111. The wiretapping facilitated by the Session Replay Codes is ongoing during each website visit and intercepts the contents of these communications between Plaintiffs and Spirit with instantaneous transmissions to the Session Replay Provider, as illustrated below, in which only 93 milliseconds were required to send a packet of event response data, which would indicate whatever the website user had just done:



112. Thus, on multiple occasions when Plaintiffs visited Spirit's website, the contents of their communications with the website were intercepted by Session Replay Code and simultaneously transmitted to Session Replay Providers.

113. The Session Replay Codes operate in the same manner for all putative Class Members.

114. Like Plaintiffs, each Class Member visited www.spirit.com with Session Replay Code embedded in it, and those Session Replay Codes intercepted the Class Members' Website Communications with www.spirit.com by sending hyper-frequent logs of those communications to Session Replay Providers.

115. Even if Spirit masks certain elements when it configures the settings of the Session Replay Code embedded on its website, any operational iteration of the Session Replay Code will, by its very nature and purpose, intercept the contents of communications between the website's visitors and the website owner.

116. For example, even with heightened masking enabled, Session Replay Providers will still learn through the intercepted data exactly which pages a user navigates to, how the user moves through the page (such as which areas the user zooms in on or interacted with), and additional substantive information.

117. The Session Replay Code procured by Spirit is an electronic, mechanical, or other analogous device in that the Session Replay Code, monitors, collects, and records the content of electronic computer-to-computer communications between Plaintiffs' mobile computer and/or mobile device and the computer servers and hardware utilized by Spirit to operate its website.

118. Additionally, the Session Replay Code is software designed to alter the operation of a website visitor's computer or mobile phone by instructing the hardware components of that physical device to run the processes that ultimately intercept the visitor's communications and transmit them to the third-party Session Replay Provider, without the visitor's knowledge.

119. The Session Replay Code procured by Spirit is not a website cookie, analytics tool, tag, web beacon, or other similar technology. Instead, the data collected by the Session Replay Code identified specific information inputted and content viewed, and thus revealed personalized and sensitive information about website visitors' Internet activity and habits. As such, by the very nature of its operation, the Session Replay Code is a device used to intercept electronic communications.

120. The Website Communications intentionally monitored, collected, and recorded by Spirit was content generated through Plaintiffs' and Class Members' use, interaction, and communication with Spirit's website relating to the substance and/or meaning of Plaintiffs' and Class Members' communications with the website, *i.e.*, mouse clicks and movements, keystrokes, search terms, information inputted by Plaintiffs and Class Members, and pages and content clicked on and viewed by Plaintiffs and Class Members. The mere fact that Spirit values this content, and monitors, intercepts and records it, confirms these communications are content that convey substance and meaning to Spirit, and in turn, any Session Replay Provider that receives the intercepted information.

121. Plaintiffs and Class Members did not provide prior consent to Spirit's interception of their Website Communications, nor could they, as the interception begins *immediately* upon arriving at www.spirit.com and/or its subpages.

122. Spirit does not ask website visitors, including Plaintiffs and Class Members, for prior consent before wiretapping their Website Communications. Indeed, Plaintiffs and Class Members have no idea upon arriving at the website that Spirit is using Session Replay Code to monitor, collect, and record their Website Communications because the Session Replay Code is seamlessly incorporated and embedded into Spirit's website.

123. Further, while Spirit maintains a purported "Cookie Banner" on its website, the Cookie Banner is insufficient for Plaintiffs to furnish prior consent. First, because the wiretapping begins the moment a website user arrives on the website, Plaintiffs had no opportunity to review the Cookie Banner before they were wiretapped and therefore had no meaningful opportunity to opt out of, or prevent, the wiretapping from occurring. Second, Session Replay code is not a cookie, much less a run-of-the mill cookie. Common cookies that consumers might be familiar

with do not engage in session replay recording or all of the features described above. Rather as the 2017 study recognized, the extent of data collected by Session Replay Code "far exceeds user expectations; text typed into forms is collected before the user submits the form, and precise mouse movements are saved, all without any visual indication to the user."[47]

124. Further, while Spirit purports to maintain a "Privacy Policy," the Privacy Policy is insufficient for Plaintiffs and Class Members to furnish prior consent. First, because the wiretapping begins the moment a website user visits www.spirit.com or one of its subpages, Plaintiffs and Class Members had no opportunity to review the Privacy Policy before they were wiretapped and therefore could not have opted out of or prevented the wiretapping before it occurred. Additionally, a reasonable person would not be on notice of the terms of Spirit's Privacy Policy by way of normal interaction with the website. Spirit's Privacy Policy is contained on the homepage of www.spirit.com, in a Cookie Banner that has nothing to do with Session Replay Code or the collection of Website Communications. As such, a reasonable person could browse for flights on Spirit's website without ever being on notice of the purported Privacy Policy.

CLASS ACTION ALLEGATIONS

125. Plaintiffs bring this action pursuant to Federal Rule of Civil Procedure 23 individually and on behalf of the following Classes:

California Class:

All natural persons in California whose Website Communications were captured through the use of Session Replay Code embedded in Defendant's website.

Maryland Class:

All natural persons in Maryland whose Website Communications were through the use of Session Replay Code embedded in Defendant's website.

[47] Englehardt, *supra* note 22.

Pennsylvania Class:

All natural persons in Pennsylvania whose Website Communications were captured through the use of Session Replay Code embedded in Defendant's website.

126. Excluded from the Classes are Defendant, its parents, subsidiaries, affiliates, officers, and directors, all persons who make a timely election to be excluded from the Classes, the judge to whom this case is assigned, and any immediate family members thereof, and the attorneys who enter their appearance in this action.

127. **Numerosity:** The members of the Classes are so numerous that individual joinder of all Class Members is impracticable. The precise number of Class Members and their identities may be obtained from the books and records of Defendant or the Session Replay Providers.

128. **Commonality:** This action involves questions of law and fact that are common to the Class Members. Such common questions include, but are not limited to:

a. whether Defendant procures Session Replay Providers to intercept Defendant's website's visitors' Website Communications;

b. whether Defendant intentionally discloses the intercepted Website Communications of its website users;

c. whether Defendant acquires the contents of website users' Website Communications without their consent;

d. whether Defendant's conduct violates California Penal Code § 631 ("CIPA"), Statutory Larceny, Cal. Pen. Code §§ 484, 496, Unfair Competition Law, Cal. Bus. & Prof. Code §§ 17200, *et seq.*, MWESA, Md. Code. Ann., Cts. & Jud. Proc. § 10-401, or WESCA, 18 Pa. C.S.A. §§ 5701, *et seq*.,

e. whether Plaintiffs and the Class Members are entitled to equitable relief; and

f. whether Plaintiffs and the Class Members are entitled to actual, statutory, punitive, or other forms of damages, and other monetary relief.

129. **Typicality:** Plaintiffs' claims are typical of the other Class Members' claims because, among other things, all Class Members were comparably injured through the uniform prohibited conduct described above. For instance, Plaintiffs and each member of the Classes had their communications intercepted in violation of the law and their right to privacy. This uniform injury and the legal theories that underpin recovery make the claims of Plaintiffs and the members of the Class typical of one another.

130. **Adequacy of Representation:** Plaintiffs have and will continue to fairly and adequately represent and protect the interests of the Classes. Plaintiffs have retained counsel competent and experienced in complex litigation and class actions, including litigations to remedy privacy violations. Plaintiffs have no interest that is antagonistic to the interests of the Classes, and Defendant has no defenses unique to Plaintiffs. Plaintiffs and their counsel are committed to vigorously prosecuting this action on behalf of the members of the Classes, and they have the resources to do so. Neither Plaintiffs nor their counsel have any interest adverse to the interests of the other members of the Classes.

131. **Superiority:** This class action is appropriate for certification because class proceedings are superior to other available methods for the fair and efficient adjudication of this controversy and joinder of all members of the Classes is impracticable. This proposed class action presents fewer management difficulties than individual litigation, and provides the benefits of single adjudication, economies of scale, and comprehensive supervision by a single court. Class

treatment will create economies of time, effort, and expense and promote uniform decision-making.

132. **Predominance:** Common questions of law and fact predominate over any questions affecting only individual Class Members. Similar or identical violations, business practices, and injuries are involved. Individual questions, if any, pale by comparison, in both quality and quantity, to the numerous common questions that dominate this action. For example, Defendant's liability and the fact of damages is common to Plaintiffs and each member of the Classes. If Defendant intercepted Plaintiffs' and Class Members' Website Communications, then Plaintiffs and each Class Member suffered damages by that conduct.

133. **Ascertainability:** Members of the Classes are ascertainable. Class Membership is defined using objective criteria, and Class Members may be readily identified through Defendant's books and records or the Session Replay Providers' books and records.

COUNT I
VIOLATION OF PENNSYLVANIA WIRETAP ACT
18 Pa. Cons. Stat. § 5701, *et. seq.*

134. Plaintiff Smidga incorporates the preceding paragraphs as if fully set forth herein.

135. Plaintiff Smidga brings this claim individually and on behalf of the Pennsylvania Class.

136. The Pennsylvania Wiretap Act (the "Act") prohibits (1) the interception or procurement of another to intercept any wire, electronic, or oral communication; (2) the intentional disclosure of the contents of any wire, electronic, or oral communication that the discloser knew or should have known was obtained through the interception of a wire, electronic, or oral communication; and (3) the intentional use of the contents of any wire, electronic, or oral communication that the discloser knew or should have known was obtained through the interception of a wire, electronic, or oral communication. 18 Pa. Cons. Stat. § 5703.

137. Any person who intercepts, discloses, or uses or procures any other person to intercept, disclose, or use, a wire, electronic, or oral communication in violation of the Act is subject to a civil action for (1) actual damages, not less than liquidated damages computed at the rate of $100/day for each violation or $1,000, whichever is higher; (2) punitive damages; and (3) reasonable attorneys' fees and other litigation costs incurred. 18 Pa. Cons. Stat. § 5725(a).

138. "Intercept" is defined as any "[a]ural or other acquisition of the contents of any wire, electronic or oral communication through the use of any electronic, mechanical or other device." 18 Pa. Cons. Stat. § 5702.

139. "Contents" is defined as "used with respect to any wire, electronic or oral communication, is any information concerning the substance, purport, or meaning of that communication." 18 Pa. Cons. Stat. § 5702.

140. "Person" is defined as "any individual, partnership, association, joint stock company, trust or corporation." 18 Pa. Cons. Stat. § 5702.

141. "Electronic Communication" is defined as "[a]ny transfer of signs, signals, writing, images, sounds, data or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photo-optical system." 18 Pa. Cons. Stat. § 5702.

142. Spirit is a person for purposes of the Act because it is a corporation.

143. Session Replay Code like that procured by Spirit is a "device" used for the "acquisition of the contents of any wire, electronic, or oral communication" within the meaning of the Act. Courts have held that software constitutes a "device" for purposes of applying wiretap statutes. *See, e.g.*, *United States v. Barrington*, 648 F.3d 1178, 1203 (11th Cir. 2011) (accepting that a keylogger software could be considered a device); *Luis v. Zang*, 833 F.3d 619, 630 (6th Cir. 2016) (accepting that a software could be a "device" for the purpose of the Wiretap Act); *In re*

Carrier IQ, Inc., 78 F. Supp. 3d 1051, 1087 (N.D. Cal. 2015) (concluding that a software was an "electronic, mechanical or other device"); *Klumb v. Goan*, 884 F. Supp. 2d 644, 661-62 (E.D. Ten. 2012) (analyzing spyware software as a device under Wiretap Act); *Shefts v. Petrakis*, 2012 WL 4049484, at *8-9 (C.D. Ill. 2012) (analyzing software as a device under the Wiretap Act).

144. Alternatively, even if the Session Replay Code itself were not considered a "device" under the Act, Spirit ultimately "uses" the physical computers and mobile phones of Plaintiff Smidga and Class Members by sending the Session Replay Code to those devices. In turn, the Session Replay Code instructs those devices to run the physical processes necessary to accomplish the interception of Plaintiff Smidga's and Class Members' communications and transmission of those communications to the third-party Session Replay Providers.

145. Spirit intentionally procures and embeds Session Replay Code on its website to spy on—automatically and secretly—and to intercept its website visitors' electronic interactions communications with Spirit in real time.

146. Plaintiff Smidga's and Class Members' intercepted Website Communications constitute the "contents" of electronic communication[s]" within the meaning of the Act.

147. Plaintiff Smidga's and Class Members' electronic communications are intercepted contemporaneously with their transmission.

148. Plaintiff Smidga's and Class Members' interactions with Spirit's website and its subpages, including their directional, selection, and clicking actions (using a mouse, arrow keys, or a finger), the display of information coming from Spirit and directed to Plaintiff Smidga, and Plaintiff Smidga's entry of text into search form fields, were all exchanges of electronic communications between Plaintiff Smidga and Spirit.

149. Plaintiff Smidga's and Class Members' intercepted Website Communications therefore constitute the "contents" of "electronic communication[s]" within the meaning of the Act.

150. By operation of the Session Replay Code on Plaintiff Smidga's device, these forms of communications were captured continuously, within milliseconds, and immediately transmitted to and acquired by third-party Session Replay Providers.

151. Plaintiff Smidga and Class Members did not consent to having their Website Communications wiretapped.

152. Pursuant to 18 Pa. Cons. Stat. 5725(a), Plaintiff Smidga and the Class Members seek (1) actual damages, not less than liquidated damages computed at the rate of $100/day for each violation or $1,000, whichever is higher; (2) punitive damages; and (3) reasonable attorneys' fees and other litigation costs incurred.

153. Spirit's conduct is ongoing, and it continues to unlawfully intercept the communications of Plaintiff Smidga and Class Members any time they visit Defendant's website with Session Replay Code enabled without their consent. Plaintiff Smidga and Class Members are entitled to declaratory and injunctive relief to prevent future interceptions of their communications.

COUNT II
INVASION OF PRIVACY – PENNSYLVANIA INTRUSION UPON SECLUSION

154. Plaintiff Smidga, individually and on behalf of the Pennsylvania Class, repeats and realleges each and every allegation contained above as if fully alleged herein.

155. Pennsylvania common law recognizes the tort of invasion of privacy. The right to privacy is also embodied in multiple sections of the Pennsylvania constitution.

156. Each time Plaintiff Smidga and Class Members visited Defendant's website on their personal computers and/or mobile devices, Defendant secretly monitored, recorded, and collected

their personal data, in real-time, for Defendant's monetary gain and without Plaintiff Smidga's and Class Members' consent.

157. Plaintiff Smidga's and Class Members' URLs, web page address information, mouse clicks and movements, scrolling, zooms (out or in), and text submissions (both partial and complete), including search terms or similar communications, were all collected by the Session Replay Code that Defendant procured and deployed on its website.

158. Plaintiff Smidga and Class Members have an objective, reasonable expectation of privacy in their Website Communications.

159. Because the data collected by the Session Replay Code identifies specific information input and content viewed by visitors to Defendant's website, it reveals personalized and sensitive information about the website visitors' Internet activity, including the visitor's personal interests, search queries, and habits.

160. Defendant's surreptitious procurement and interception of website visitors' Website Communications therefore allowed Defendant to monitor, record, and disclose Plaintiff Smidga's and Class Members' personal interests, browsing histories, search queries, and habits as they interacted with and browsed Defendant's website in real-time.

161. Upon information and belief, the Session Replay Code embedded on Defendant's website indiscriminately captures the maximum range of data and information, including highly sensitive and personal information displayed by the websites.

162. Plaintiff Smidga and Class Members did not consent to, authorize, or know about Defendant's intrusion at the time it occurred. Plaintiff Smidga and Class Members never agreed that Defendant could collect, disclose, or use the contents of their Website Communications.

163. Plaintiff Smidga and Class Members had an objective interest in precluding the dissemination and/or misuse of their information and communications and in conducting their personal activities without intrusion or interference, including the right to not have their personal information intercepted and utilized for business gain.

164. Defendant intentionally intrudes on Plaintiff Smidga's and Class Members' private life, seclusion, or solitude, without consent.

165. Defendant's conduct is highly objectionable to a reasonable person and constitutes an egregious breach of the social norms underlying the right to privacy.

166. Defendant deprived Plaintiff Smidga and Class Members of the right to control how their personal information and communications are received, used, or disseminated and by whom.

167. Plaintiff Smidga and Class Members were harmed by Defendant's wrongful conduct as Defendant's conduct has caused Plaintiff Smidga and the Class mental anguish and suffering arising from their loss of privacy and confidentiality of their personal information.

168. Defendant's conduct has needlessly harmed Plaintiff Smidga and the Class by capturing intimately personal facts and data in the form of their Website Communications. This disclosure and loss of privacy and confidentiality has caused Plaintiff Smidga and the Class to experience mental anguish, emotional distress, worry, fear, and other harms.

169. Additionally, given the monetary value of individual personal information, Defendant deprived Plaintiff Smidga and Class Members of the economic value of their interactions with Defendant's website, without providing proper consideration for Plaintiff Smidga's and Class Members' property.

170. Further, Defendant has improperly profited from their invasion of Plaintiff Smidga's and Class Members' privacy by using Plaintiff Smidga's and Class Members' personal data and information for its economic value and Defendant's own commercial gain.

171. Upon information and belief, Defendant derives a significant benefit from the content intercepted through its procurement and use of Session Replay Code, by collecting, retaining, and using that data and information to maximize profits through predictive marketing and other targeted advertising practices.

172. As a direct and proximate result of Defendant's conduct, Plaintiff Smidga and Class Members are entitled to damages, including compensatory, punitive, and/or nominal damages, in an amount to be proven at trial.

173. Defendant's conduct is ongoing. Defendant continues to unlawfully procure the interception and to unlawfully intercept the Website Communications of Plaintiff Smidga and Class Members any time they visit Defendant's website with Session Replay Code enabled without their consent. Plaintiff Smidga and Class Members are entitled to declaratory and injunctive relief to prevent future interceptions of their communications.

COUNT III
VIOLATION OF MARYLAND WIRETAP ACT
Md. Code Ann., Cts. & Jud. Proc. § 10-401, *et. seq.*

174. Plaintiff Curd incorporates paragraphs 1 to 133 as if fully set forth herein.

175. Plaintiff Curd brings this claim individually and on behalf of the Maryland Class.

176. The Maryland Wiretap Act (the "Act") prohibits (1) the interception or procurement of another to intercept any wire, electronic, or oral communication; (2) the willful disclosure of the contents of any wire, electronic, or oral communication that the discloser knew or should have known was obtained through the interception of a wire, electronic, or oral communication; and (3) the willful use of the contents of any wire, electronic, or oral communication that the discloser

knew or should have known was obtained through the interception of a wire, electronic, or oral communication. Md. Code Ann., Cts. & Jud. Proc. § 10-402.

177. Any person who intercepts, discloses, or uses or procures any other person to intercept, disclose, or use, a wire, electronic, or oral communication in violation of the Act is subject to a civil action for (1) actual damages, not less than liquidated damages computed at the rate of $100/day for each violation or $1,000, whichever is higher; (2) punitive damages; and (3) reasonable attorneys' fees and other litigation costs incurred. Md. Code Ann., Cts. & Jud. Proc. § 10-410(a).

178. "Intercept" is defined as any "aural or other acquisition of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device." Md. Code Ann., Cts. & Jud. Proc. § 10-401(10).

179. "Contents" is defined as when "used with respect to any wire, oral, or electronic communication, includes any information concerning the identity of the parties to the communication or the existence, substance, purport, or meaning of that communication." Md. Code Ann., Cts. & Jud. Proc. § 10-401(4).

180. "Person" is defined as, in relevant part "any individual, partnership, association, joint stock company, trust, or corporation." Md. Code Ann., Cts. & Jud. Proc. § 10-401(14).

181. "Electronic Communication" is defined as "any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic, or photooptical system." Md. Code Ann., Cts. & Jud. Proc. § 10-401(5)(i).

182. Spirit is a person for purposes of the Act because it is a corporation.

183. Session Replay Code like that procured by Spirit is a "device" used for the "acquisition of the contents of any wire, electronic, or oral communication" within the meaning of the Act.

184. Plaintiff Curd's and Class Members' intercepted Website Communications constitute the "contents" of electronic communications within the meaning of the Act.

185. Spirit willfully procures and embeds Session Replay Code on its website to spy on, automatically and secretly, and intercept its website visitors' electronic interactions communications with Spirit in real time.

186. Plaintiff Curd's and Class Members' electronic communications are intercepted contemporaneously with their transmission.

187. Plaintiff Curd and Class Members did not consent to having their Website Communications wiretapped.

188. Pursuant to Md. Code Ann., Cts. & Jud. Proc. § 10-410, Plaintiff Curd and the Class Members seek (1) actual damages, not less than liquidated damages computed at the rate of $100/day for each violation or $1,000, whichever is higher; (2) punitive damages; and (3) reasonable attorneys' fees and other litigation costs incurred.

189. Spirit's conduct is ongoing, and it continues to unlawfully intercept the communications of Plaintiff Curd and Class Members any time they visit Defendant's website with Session Replay Code enabled without their consent. Plaintiff Curd and Class Members are entitled to declaratory and injunctive relief to prevent future interceptions of their communications.

COUNT IV
INVASION OF PRIVACY – INTRUSION UPON SECLUSION

190. Plaintiff Curd, individually and on behalf of the Maryland Class, repeats and realleges paragraphs 1 to 133 and paragraphs 174 to 189 contained above as if fully alleged herein.

191. Maryland common law recognizes the tort of invasion of privacy.

192. Plaintiff Curd and Class Members have an objective, reasonable expectation of privacy in their Website Communications.

193. In violation of Plaintiff Curd's and Class Members' reasonable expectation of privacy, Defendant intentionally procured and embedded Session Replay Code on its website to intercept and record Plaintiff Curd's and Class Members' every move.

194. Defendant willfully intruded on Plaintiff Curd's and Class Members' private lives, seclusion and solitude, by, for all intents and purposes, installing a recording device on their web browsers without their consent.

195. Each time Plaintiff Curd and Class Members visited Defendant's website on their personal computers and/or mobile devices, the Session Replay Code procured and utilized by Defendant secretly collected their personal data in real-time for Defendant's monetary gain and without their consent.

196. Because the data collected by the Session Replay Code identifies specific information inputted and content viewed by visitors to Defendant's website, it reveals personalized and sensitive information about the website visitors' internet activity, including the visitor's personal interests, search queries, and habits.

197. Defendant's surreptitious interception of website visitors' Website Communications therefore allowed Defendant to monitor, record, and disclose Plaintiff Curd's

and Class Members' personal interests, browsing histories, search queries, and habits as they interacted with and browsed Defendant's website in real-time.

198. Upon information and belief, the Session Replay Code embedded on Defendant's websites indiscriminately captures the maximum range of data and information, including highly sensitive and personal information displayed by the websites.

199. Plaintiff Curd and Class Members did not consent to, authorize, or know about Defendant's procurement of Session Replay Code or intrusion at the time it occurred. Plaintiff Curd and Class Members never agreed that Defendant could collect, disclose, or use the contents of their Website Communications.

200. Plaintiff Curd and Class Members had an objective interest in precluding the dissemination and/or misuse of their information and communications and in conducting their personal activities without intrusion or interference, including the right to not have their personal information intercepted and utilized for business gain.

201. Defendant willfully intrudes on Plaintiff Curd's and Class Members' private life, seclusion, or solitude, without consent.

202. Defendant's conduct is highly objectionable to a reasonable person and constitutes an egregious breach of the social norms underlying the right to privacy.

203. Defendant deprived Plaintiff Curd and Class Members of the right to control how their personal information and communications are received, used, or disseminated and by whom.

204. Plaintiff Curd and Class Members were harmed by Defendant's wrongful conduct as Defendant's conduct has caused Plaintiff Curd and the Class mental anguish and suffering arising from their loss of privacy and confidentiality of their electronic communications.

205. Defendant's conduct has needlessly harmed Plaintiff Curd and the Class by capturing intimately personal facts and data in the form of their Website Communications. This intrusion, disclosure of information, and loss of privacy and confidentiality has caused Plaintiff Curd and the Class to experience mental anguish, emotional distress, worry, fear, and other harms.

206. Additionally, given the monetary value of individual personal information, Defendant deprived Plaintiff Curd and Class Members of the economic value of their interactions with Defendant's website, without providing proper consideration for Plaintiff Curd's and Class Members' property.

207. Further, Defendant has improperly profited from its invasion of Plaintiff Curd's and Class Members' privacy in their use of their data for its economic value and Defendant's own commercial gain.

208. Upon information and belief, Defendant derives significant benefit from the content intercepted through its procurement and use of Session Replay Code, by collecting, retaining, and using that data and information to maximize profits through predictive marketing and other targeted advertising practices.

209. As a direct and proximate result of Defendant's conduct, Plaintiff Curd and Class Members are entitled to damages, including compensatory, punitive, and/or nominal damages, in an amount to be proven at trial.

210. Defendant's conduct is ongoing. Defendant continues to unlawfully procure the interception of and intercept the Website Communications of Plaintiff Curd and Class Members any time they visit Defendant's website with Session Replay Code enabled without their consent. Plaintiff Curd and Class Members are entitled to declaratory and injunctive relief to prevent future interceptions of their communications.

COUNT V
VIOLATION OF CALIFORNIA INVASION OF PRIVACY ACT
Cal. Penal Code § 630 *et. seq.*

211. Plaintiff Mandeng incorporates paragraphs 1 to 133 by reference as if fully set forth herein and brings this count individually and on behalf of the California Class.

212. The California Invasion of Privacy Act ("CIPA") is codified at Cal. Penal Code §§ 630-638. The Act contains the following statement of purpose:

> The Legislature hereby declares that advances in science and technology have led to the development of new devices and techniques for the purpose of eavesdropping upon private communications and that the invasion of privacy resulting from the continual and increasing use of such devices and techniques has created a serious threat to the free exercise of personal liberties and cannot be tolerated in a free and civilized society.

213. California Penal Code § 631(a) accordingly provides, in pertinent part:

> Any person who, by means of any machine, instrument, or contrivance, or in any other manner . . . willfully and without the consent of all parties to the communication, or in any unauthorized manner, reads, or attempts to read, or to learn the contents or meaning of any message, report, or communication while the same is in transit or passing over any wire, line, or cable, or is being sent from, or received at any place within this state; or who uses, or attempts to use, in any manner, or for any purpose, or to communicate in any way, any information so obtained, or who aids, agrees with, employs, or conspires with any person or persons to unlawfully do, or permit, or cause to be done any of the acts or things mentioned above in this section, is punishable by a fine not exceeding two thousand five hundred dollars ($2,500).

214. At all relevant times, Spirit's business practice of injecting Session Replay Code allowed it to access, intercept, learn the contents of and collect Plaintiff Mandeng's and Class Members' personally identifiable information and other data.

215. Plaintiff Mandeng, and each Class Member, visited and/or interacted with the Spirit website while in California.

216. Plaintiff Mandeng and Class Members did not consent to any of Spirit's actions in intercepting, reading, and learning the contents of their communications.

217. Spirit's conduct was intentional in that it purposefully installed code which allows it to eavesdrop and learn the content of its users' communications and other browsing activities that would otherwise be unavailable to Spirit without engaging in this practice. Spirit directly participated in the interception, reading, and/or learning of the contents of the communications between Plaintiff Mandeng, Class Members and California-based web entities.

218. The information Spirit intercepts while Plaintiff Mandeng and Class Members are using its website includes personally identifiable information and other highly specific information and communications, including, without limitation, every button, keystroke and link a user taps, whether the user has taken any screenshots, text entries (including passwords and credit card information), and how much time a user spent on the website.

219. Plaintiff Mandeng and Class Members have suffered loss by reason of these violations, including but not limited to, violation of the right to privacy. Unless restrained and enjoined, Spirit will continue to commit such acts.

220. As a result of the above violations and pursuant to CIPA § 637.2, Spirit is liable to Plaintiff Mandeng and Class Members for the greater of treble actual damages related to their loss of privacy in an amount to be determined at trial or for statutory damages in the amount of $5,000 per violation. Section 637.2 provides "[it] is not a necessary prerequisite to an action pursuant to this section that the plaintiffs has suffered, or be threatened with, actual damages."

221. Plaintiff Mandeng further requests, as provided under CIPA, reasonable attorneys' fees and costs of suit, injunctive and declaratory relief, and punitive damages in an amount to be determined by a jury sufficient to prevent or deter the same or similar conduct by Spirit.

COUNT VI
STATUTORY LARCENY
Cal. Pen. Code §§ 484 AND 496

222. Plaintiff Mandeng, individually and on behalf of the California Class, repeats and realleges paragraphs 1 to 133 and paragraphs 211 to 221 contained above as if fully alleged herein.

223. California Penal Code § 496(a) prohibits the obtaining of property "in any manner constituting theft." California Penal Code § 484 defines theft:

> Every person who shall feloniously steal, take, carry, lead, or drive away the personal property of another, or who shall fraudulently appropriate property which has been entrusted to him or her, or who shall knowingly and designedly, by any false or fraudulent representation or pretense, defraud any other person of money, labor or real or personal property, or who causes or procures others to report falsely of his or her wealth or mercantile character and by thus imposing upon any person, obtains credit and thereby fraudulently gets or obtains possession of money, or property or obtains the labor or service of another, is guilty of theft.

224. Accordingly, the Cal. Pen. Code, specifically, Section 484, definition of "theft" includes obtaining property by false pretenses and provides the basis for a privacy right of action.

225. Defendant intentionally employed a program procured from third parties that would obtain personal private information under a false purpose, through deception and without the knowledge of Plaintiff Mandeng or the Class Members, and in doing so, deceived Plaintiff Mandeng and California Class Members into providing information to Defendant and by extension to the Session Replay Providers.

226. Defendant stole, took, and/or fraudulently appropriated Plaintiff Mandeng's and Class Members' personal information without their consent.

227. Defendant concealed, aided in the concealing, sold, and/or utilized Plaintiff Mandeng's and Class Members' personal information obtained for Defendant's commercial purposes and the financial benefit of Defendant.

228. Defendant knowingly and intentionally committed the acts wherein it obtained by false pretense personal information because Defendant intentionally deployed the Session Replay Code that tracked Plaintiff Mandeng's and Class Members' information and operated it in a manner that was concealed and/or withheld from Plaintiff Mandeng and Class Members.

229. Defendant deprived Plaintiff Mandeng and Class Members of the right to control how their personal information and communications are received, used, or disseminated and by whom.

230. With fraudulent intent, Defendant concealed, aided in the concealing, and/or utilized Plaintiff Mandeng's and the Class Members' information for commercial purposes and to Defendant's direct financial benefit, as the reasonable and fair market value of the unlawfully obtained data can be determined in the marketplace.

231. Plaintiff Mandeng and Class Members are entitled to recover the reasonable and fair market value of the unlawfully obtain personal data taken in violation of California Penal Code §§ 484 and 496.

COUNT VII
VIOLATION OF THE UNFAIR COMPETITION LAW,
Cal. Bus. & Prof. Code, Sections 17200, *et seq*.,

232. Plaintiff Mandeng, individually and on behalf of the California Class, repeats and realleges paragraphs 1 to 133 and paragraphs 211 to 231 contained above as if fully alleged herein.

233. California's Unfair Competition Law ("UCL"), Cal. Bus. & Prof. Code §§ 17200, *et seq.*, prohibits unfair competition – meaning any unlawful, unfair, or fraudulent business act or

practice; any unfair, deceptive, untrue, or misleading advertising; and any act prohibited under Business and Professions Code 17500.

234. Defendant is a "person" as defined by Cal. Bus. & Prof. Code § 17201.

235. Defendant's unlawful, unfair, and/or fraudulent business acts and practices, Defendant engaged in acts of unlawful and/or unfair competition prohibited by Business and Professions Code 17200 *et seq*. by virtue of the acts described herein, each of which constitutes an unlawful and/or unfair business practice. The use of such unlawful and/or unfair business practices constitutes unfair competition within the meaning of Business and Professions Code.

236. The unlawful and/or unfair business practices committed by the Defendant include, but are not limited to:

a. Committing trespass to chattels;

b. Committing conversion to chattels;

c. Committing civil trespass;

d. Violating California common law;

e. Violating federal and state statutory laws;

f. Violating the FTC Act and FTC directives;

g. Engaging in conduct in which the gravity of the harm to Plaintiff Mandeng and the Class outweighs the utility of the Defendant's conduct;

h. Engaging in acts and/or practices and/or omissions that are immoral, unethical, oppressive, or unscrupulous and causes injury to consumers which outweigh its benefits;

i. Without Plaintiff Mandeng's or Class Members' knowledge or consent, Defendant injected code into its website that was capable of transmitting the

substance of Plaintiff Mandeng's and Class Members' communications with Defendant to unauthorized third parties and actively aided and abetted the interception, viewing, and collection of Plaintiff Mandeng's and Class Members' personal information and communications so that they could be used for advertising and other purposes for Defendant's financial benefit. The information and data Defendant intercepted includes valuable personal information, including but not limited to personally identifiable information and other privileged communications and facts; and

j. Failing to disclose Defendant's practices prior to implementing Session Replay Code.

237. Plaintiff Mandeng and Class Members interacted with Defendant's website reasonably believing that their browsing activities—and any facts and information communicated to Defendant's website—were secure and confidential (*i.e.*, solely between themselves and Defendant).

238. The fact that Defendant shared the personal information of its website's visitors with the Session Replay Providers is material information and Plaintiff Mandeng and Class Members would not have used the website, or insisted on better privacy controls, had Defendant disclosed this information.

239. There is no justification for Defendant's conduct other than to increase, beyond what it would have otherwise realized, its profit from the value of its information assets through the interception and acquisition of Plaintiff Mandeng's and Class Members' personal information. Defendant's conduct lacks justification in that Defendant has benefited from such conduct and practices while Plaintiff Mandeng and Class Members have been misled as to the nature and

integrity of Defendant's services and have, in fact, suffered material disadvantage regarding their interests in the privacy and confidentiality of their personal information.

240. Defendant actively concealed its tracking practices at issue and had exclusive knowledge of it, creating a duty to disclose. Defendant could have disclosed its use of Session Replay Code and obtained its website visitor's affirmative consent.

241. Defendant failed to disclose this tracking practice. Its disclosure would have been a material and important factor in Plaintiff Mandeng's and Class Members' actions related to their use of the website.

242. Defendant's secret, undisclosed, and deceptive tracking practice caused Plaintiff Mandeng and Class Members to surrender more in their transactions with Defendant than they otherwise would have. Had Plaintiff Mandeng and Class Members known that Defendant could and would use their in-app browser in the manner described, they would have avoided using the website or demanded better privacy controls, thereby avoiding this injury.

243. Defendant's conduct was immoral, unethical, oppressive, unscrupulous, and substantially injurious to Plaintiff Mandeng and Class Members. Further, Defendant's conduct narrowly benefited their own business interests at the expense of Plaintiff Mandeng's and Class Members' fundamental privacy interests protected by statute, the California Constitution, and the common law.

244. Plaintiff Mandeng's and Class Members' loss of their personal information constitutes an economic injury.

245. Plaintiff Mandeng and Class Members have suffered harm in the form of lost property value, specifically the diminution of the value of their private and personally identifiable data and content.

246. Defendant's actions caused damage to and loss of Plaintiff Mandeng's and Class Members' property right to control the dissemination and use of their personal information and communications.

247. Plaintiff Mandeng and Class Members have a property right in their personal information, which has value to themselves as well as Defendant, and lost money or property as a result of Defendant's violations of the UCL.

248. Each and every separate act constitutes an unlawful and/or unfair business practice. Each day that Defendant engaged in each separate unlawful act, omission, or practice is a separate and distinct violation of Business and Professions Code § 17200.

249. As a direct and proximate result of the foregoing acts and practices, Defendant has received income, profits, and other benefits, which it would not have received if Defendant had not engaged in the violations of the Unfair Competition Law described in this Complaint.

250. As a direct and proximate result of the foregoing acts and practices, Defendant has obtained a competitive unfair advantage over similar businesses that have not engaged in such practices.

251. Plaintiff Mandeng has no adequate remedy at law in that damages are insufficient to protect the public from the harm caused by the conditions described in this Complaint.

252. Plaintiff Mandeng and Class Members desire to continue using Defendant's website, but unless injunctive relief is granted to enjoin the unlawful business practices of Defendant, Plaintiff Mandeng, the Class, and the general public have no confidence that Defendant will not continue to share their personal information and substantive communications with third parties and will suffer irreparable injury and damage.

253. Plaintiff Mandeng and the Class have suffered injury in fact as a result of Defendant's unlawful, unfair, and/or fraudulent acts and/or practices.

254. Plaintiff Mandeng seeks to enjoin further unlawful, unfair, and/or fraudulent acts or practices by Defendant, under Cal. Bus. & Prof. Code § 17200.

255. Plaintiff Mandeng requests that this Court enter such orders or judgments as may be necessary to enjoin Defendant from continuing its acts and/or practices which violate the UCL and to restore to Plaintiff Mandeng and Class Members any money Defendant acquired by unfair competition, including restitution and/or restitutionary disgorgement, as provided in Cal. Bus. & Prof. Code § 17203 and Cal. Civ. Code § 3345; and for such other relief set forth below.

COUNT VII
TRESPASS TO CHATTELS

256. Plaintiffs repeat and reallege each and every allegation contained above as if fully alleged herein. For purposes of this Count, "Plaintiffs and the Classes" means Plaintiffs and the California, Maryland, and Pennsylvania and Classes.

257. Plaintiffs and the Classes owned, possessed, and/or had a right to possess Plaintiffs' devices (*i.e.*, their mobile device or computer) and/or the data contained therein.

258. Plaintiffs' and Class Members' devices are chattel in that the devices are tangible, movable, and transferable.

259. Plaintiffs' and Class Members' data is also valuable chattel that is tangible or intangible and is movable and transferable.

260. As set forth above, Defendant intentionally, directly or through a third party, interfered with; intermeddled with; used; took; transferred from Plaintiffs and the Classes; and/or exercised control or authority inconsistent with Plaintiffs' and Class Members' use and/or possession of the data contained on Plaintiffs' devices as described above.

261. As to the devices, Defendant used Plaintiffs' and Class Members' devices by causing a third party to place Session Replay Code directly on Plaintiffs' and the Classes devices for the purpose of tracking all of the user's interactions with the website that it would not have been able to track had it not placed the Session Replay Code on the device and engaged in this surreptitious tracking. Defendant caused a third party to transfer Plaintiffs' data from Plaintiffs' devices to the cloud storage data centers of the Session Replay Providers. Defendant exercised control or authority inconsistent with Plaintiffs' and Class Members' use and/or possession of the devices by placing the Session Replay Code to stalk users of their websites.

262. As to the data, Defendant used Plaintiffs' and Class Members' data by transferring it from Plaintiffs' device to the cloud storage data centers of the Session Replay Providers for the purpose of using the data to make money without paying for it. Defendant exercised control or authority inconsistent with Plaintiffs' and Class Members' use and/or possession of the data by capturing, taking, and/or using the data without permission or consent from Plaintiffs and the Classes.

263. Plaintiffs' data that was transferred from Plaintiffs' and Class Members' respective devices are maintained in cloud storage devices located on servers across the nation.

264. All Session Replay Providers operate in a similar manner with cloud devices and servers.

265. Plaintiffs and the Classes did not consent to the aforementioned intermeddling and/or interference.

266. The aforementioned intermeddling and/or interference was the actual and proximate cause of injury to Plaintiffs and the Classes because it exposed their respective private data and/or personally identifiable information and/or other data to one or more third parties.

267. Additionally, the interference gave third parties the data and information without the consent of Plaintiffs and the Classes and which is valuable and for which Defendant did not obtain informed consent nor pay Plaintiffs or the Classes to obtain.

268. Plaintiffs and the Class Members are entitled to recover the actual damages they suffered as a result of Defendant's aforementioned interference with their respective computer and/or mobile devices in an amount to be determined at trial.

COUNT VIII
CONVERSION TO CHATTELS

269. Plaintiffs repeat and reallege each and every allegation contained above as if fully alleged herein. For purposes of this Count, "Plaintiffs and the Classes" or "Plaintiffs and Class Members" means Plaintiffs and the California, Maryland, and Pennsylvania Classes.

270. Plaintiffs and the Classes owned, possessed, and/or had a right to possess Plaintiffs' devices (*i.e.*, their mobile device or computer) and/or the data contained therein.

271. Plaintiffs' and Class Members' devices are chattel in that the devices are tangible, movable, and transferrable.

272. Plaintiffs' and Class Members' data is also valuable chattel that is tangible or intangible and is movable and transferable.

273. As set forth above, Defendant intentionally, directly or through a third party, interfered with; intermeddled with; used; took; transferred from Plaintiffs and the Classes; and/or exercised control or authority inconsistent with Plaintiffs' and Class Members' use and/or possession of the data contained on Plaintiffs' devices as described above.

274. As to the devices, Defendant used Plaintiffs' and Class Members' devices by placing Session Replay Code directly on Plaintiffs' and the Classes devices for the purpose of tracking all of the user's interactions with the website that it wouldn't have been able to track had

it not placed the Session Replay Code on the device and engaged in this surreptitious tracking. Session Replay Code embedded by Defendant transferred Plaintiffs' data from Plaintiffs' device to the cloud storage data centers of the Session Replay Providers. Defendant exercised control or authority inconsistent with Plaintiffs' and Class Members' use and/or possession of the devices by placing the Session Replay Code to stalk users of their websites.

275. As to the data, Defendant used Plaintiffs' and Class Members' data by transferring it from Plaintiffs' device to the cloud storage data centers of the Session Replay Providers for the purpose of using the data to make money without paying for the valuable data. Defendant exercised control or authority inconsistent with Plaintiffs' and Class Members' use and/or possession of the data by capturing, taking, and/or using the data without permission or consent from Plaintiffs and the Classes.

276. Plaintiffs' data that was transferred from Plaintiffs' and Class Members' respective devices are maintained in cloud storage devices located on servers across the nation.

277. All Session Replay Providers operate in a similar manner with cloud devices and servers.

278. As set forth above, Defendant exercised dominion and ownership over Plaintiffs' and Class Members' personally inconsistent with, and in denial of, the rights of Plaintiffs' and the Classes.

279. Plaintiffs and the Classes did not consent to the aforementioned interference.

280. The aforementioned interference was the actual and proximate cause of injury to Plaintiffs and the Classes because it exposed their respective private data and/or personally identifiable information and/or other data to one or more third parties.

281. Additionally, the interference gave third parties the data and information without

the consent of Plaintiffs and the Classes, and which is valuable, and for which Defendant did not obtain informed consent nor pay Plaintiff or the Classes to obtain.

282. Plaintiffs and the Classes are entitled to recover the actual damages they suffered as a result of Defendant's aforementioned interference with their respective devices and/or data in an amount to be determined at trial.

REQUEST FOR RELIEF

Plaintiffs, individually and on behalf of the other members of the proposed Classes, respectfully request that the Court enter judgment in Plaintiffs' and the Classes' favor and against Defendant as follows:

A. Certifying the Classes and appointing Plaintiffs as Class representatives;

B. Appointing Plaintiffs' counsel as class counsel;

C. Declaring that Defendant's past conduct was unlawful, as alleged herein;

D. Declaring Defendant's ongoing conduct is unlawful, as alleged herein;

E. Enjoining Defendant from continuing the unlawful practices described herein, and awarding such injunctive and other equitable relief as the Court deems just and proper;

F. Awarding Plaintiffs and the Class Members statutory, actual, compensatory, consequential, punitive, and nominal damages, as well as restitution and/or disgorgement of profits unlawfully obtained;

G. Awarding Plaintiffs and the Class Members pre-judgment and post-judgment interest;

H. Awarding Plaintiffs and the Class Members reasonable attorneys' fees, costs, and expenses; and

I. Granting such other relief as the Court deems just and proper.

DEMAND FOR JURY TRIAL

Plaintiffs, on behalf of themselves and the Classes, demand a trial by jury of any and all issues in this action so triable of right.

Dated: August 21, 2023

Respectfully submitted,

/s/ Gary F. Lynch

Gary F. Lynch
Kelly K. Iverson
Jamisen A. Etzel
Elizabeth Pollock-Avery
Nicholas A. Colella
Patrick D. Donathen
LYNCH CARPENTER, LLP
1133 Penn Avenue, 5th Floor
Pittsburgh, Pennsylvania 15222
Telephone: 412-322-9243
Facsimile: 412-231-0246
gary@lcllp.com
kelly@lcllp.com
jamisen@lcllp.com
elizabeth@lcllp.com
nickc@lcllp.com
patrick@lcllp.com

Katrina Carroll
LYNCH CARPENTER, LLP
111 W. Washington St.
Suite 1240
Chicago IL 60602
312.750.1265
katrina@lcllp.com

Jonathan M. Jagher
FREED KANNER LONDON & MILLEN LLC
923 Fayette Street
Conshohocken, PA 19428
610.234.6486
jjagher@fklmlaw.com

Steven M. Nathan
HAUSFELD LLP
33 Whitehall Street
Fourteenth Floor
New York, NY 10004
Telephone: (646) 357-1100
Email: snathan@hausfeld.com

James J. Pizzirusso
HAUSFELD LLP
888 16th Street N.W.
Suite 300
Washington, D.C. 20006
Telephone: (202) 540-7200
Email: jpizzirusso@hausfeld.com

Stephen B. Murray
Stephen B. Murray, Jr
Arthur M. Murray
Thomas M. Beh
THE MURRAY LAW FIRM
701 Poydras Street, Suite 4250
New Orleans, Louisiana 70139
Telephone: (504) 525-8100
Email: Tbeh@Murray-lawfirm.com

Counsel for Plaintiffs and the Proposed Classes